Gigamon Containerized Broker Configuration Guide

GigaVUE Cloud Suite

Product Version: 5.12

Document Version: 1.0

(See Change Notes for document updates.)

Gigamon Inc.
3300 Olcott Street
Santa Clara, CA 95054
408.831.4000

Change Notes

When a document is updated, the document version number on the cover page will indicate a new version and will provide a link to this Change Notes table, which will describe the updates.

Product Version	Document Version	Date Updated	Change Notes
5.12.00	1.0	04/15/2021	Configure mTLS authentication and Configure GCB for Service Mesh and HTTPS/2 Support with Metadata through GigaVUE-FM GUI topics are added.

Contents

Gigamon Containerized Broker

Gigamon Containerized Broker (GCB) is a containerized component that provides the network broker features in a containerized form. GCB can perform traffic acquisition, aggregation, basic filtering, replication, and tunneling with encryption support. GCB can be deployed in its own POD as a Kubernetes service where your workloads are running. There are various components based on multiple scenarios and requirements that the GCB receives the traffic from.

This guide provides an overview of Gigamon Containerized Broker and describes how to install and deploy GCB components in your PODs.

Topics:

About Gigamon Containerized Broker

The Gigamon Containerized Broker (GCB) is a containerized component that provides the network broker features in a containerized form. The GCB is deployed by Kubernetes orchestrator and not by GigaVUE-FM.

GCB initiates the traffic acquisition process with GCB PODs and enhances the support of the features.

Following are the modules implemented in GCB:

- **Traffic Acquisition using CNI Modules**: GCB supports traffic acquisition by reading the traffic from the Container Network Interface (CNI) modules like AWS ENI, Calico, and Flannel. During initialization, GCB receives the configuration information from the Gigamon's YAML file. Kubernetes CNI (Container Network Interface) supports any combination of ingress, egress, and management process. Following the specifications defined in the YAML file, GCB configures itself on your worker node to acquire traffic .

  > **NOTE:** After GCB registration, you cannot change the number of CNI, and CNI types. If required, a new GCB instance configured and registered.

- **Traffic Aggregation** - When GCB is running in its own POD, GCB itself serves as a traffic aggregator.
- **Filtering Module** - GCB allows basic filtering, forwarding policy, and enrichment. GCB's filtering can be passed from the YAML file and it is based upon the protocol. The selected filter cannot be changed after starting the GCB.
- **Tunneling Modules** - GCB supports L2GRE and VXLAN tunneling modules.
- **Encryption Module** - GCB maintains the required certificates to support TLS and HTTPS encryption.

Interaction between GCB and GigaVUE-FM

Following are the interaction between GCB and GigaVUE-FM:

GCB Registration

When GCB comes up in the Kubernetes environment, GCB registers itself with GigaVUE-FM. When GigaVUE-FM is unreachable, GCB tries to connect with five retries of increasing time periods. Kubernetes deployment of GCB fails, if GigaVUE-FM is unreachable even after the retries. GCB only supports IPv4 protocol.

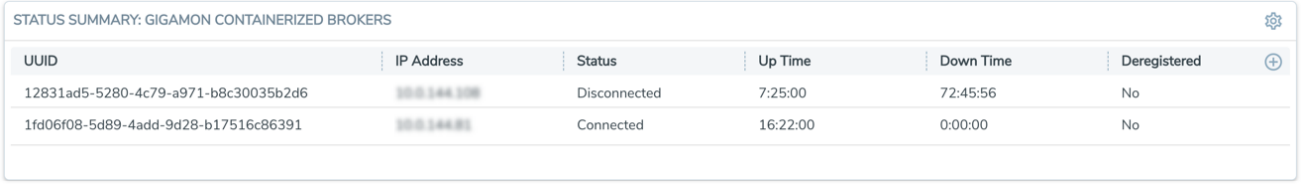
GCB Deregistration

When GCB is terminated normally, GCB sends the deregistration message to GigaVUE-FM. If GCB goes down abnormally, it might not get deregistered. The GCB PODs associated to a GCB node might then get moved to other GCB node. Similarly, if a GCB goes down, the feeding G-vTAPs are moved to other GCB, then GigaVUE-FM doesn't store GCB POD's information.

GCB Heartbeats

GCB periodically sends heartbeats to GigaVUE-FM. By default, the status of GCB is marked as **Connected**. Following are the status situations where the GCB status changes.

- If the heartbeats are missed 3 times in a row, GigaVUE-FM marks the status as **Disconnected**.
- If the heartbeats are missed 2 times in a row, GigaVUE-FM marks the status as **Pending**.
- If GigaVUE-FM doesn't receive GCB heartbeat for 30 days, then GigaVUE-FM removes the GCB, considering it as stale.


STATUS SUMMARY: GIGAMON CONTAINERIZED BROKERS

UUID	IP Address	Status	Up Time	Down Time	Deregistered
12831ad5-5280-4c79-a971-b8c30035b2d6	[redacted]	Disconnected	7:25:00	72:45:56	No
1fd06f08-5d89-4add-9d28-b17516c86391	[redacted]	Connected	16:22:00	0:00:00	No

GCB Stats

GCB sends its traffic statistics and its associated GCB PODs to GigaVUE-FM. The highest traffic and lowest traffic widgets in GigaVUE-FM dashboard shows the details of 10 highest and 10 lowest GCB traffic statistics.

GCB continues to send the stats even when there is no traffic flowing. The GCB stats are not stored in cache even if GigaVUE-FM is not reachable by GCB at that instant of time.

Monitoring Domain and Traffic Policy Configuration

You can configure and manage the Monitoring Domains, Traffic Policies, Connections, F5 fields, and Source Inventories of GCB in GigaVUE-FM. Refer to the *GigaVUE-FM REST API Reference* for detailed information on the REST APIs of GCB.

- A Traffic Policy is a combination of Rules and Tunnels.
- A rule contains specific filtering criteria that the packets must match. The filtering criteria lets you determine the target instances and the (egress or ingress) direction of tapping the network traffic.
- A tunnel is a communication path in which the traffic matching the filtered criteria is routed to the destination.

The following table provides the list of actions and their respective REST API example values.

Action	REST API and Example Value
Create a Monitoring Domain	**POST:** /cloud/monitoringDomains
Create a Connection	**POST:** /cloud/kubernetesGcb/connections
Create a Source Inventory	**POST:** /cloud/kubernetesGcb/inventory/pods/{connectionId}
Adding F5 fields information	**POST:** /cloud/kubernetesGcb/trafficPolicies/f5FieldNames
Create a Traffic Policy	**POST:** /cloud/kubernetesGcb/trafficPolicies

Action	REST API and Example Value
Redeploy a Traffic Policy	**PUT:** /cloud/kubernetesGcb/trafficPolicies/redeploy/{name}
Update a Traffic Policy	**PUT:** /cloud/kubernetesGcb/trafficPolicies/{name}
Get a Traffic Policy	**PUT:** /cloud/kubernetesGcb/trafficPolicies/status/{name}
Delete a Traffic Policy	**DELETE:** /cloud/kubernetesGcb/trafficPolicies/{name}
Delete a Connection	**DELETE:** /cloud/kubernetesGcb/connections/{id}
Delete a Monitoring Domain	**DELETE:** /cloud/monitoringDomains/{id}

Gigamon Containerized Broker for Cloud Object Storage

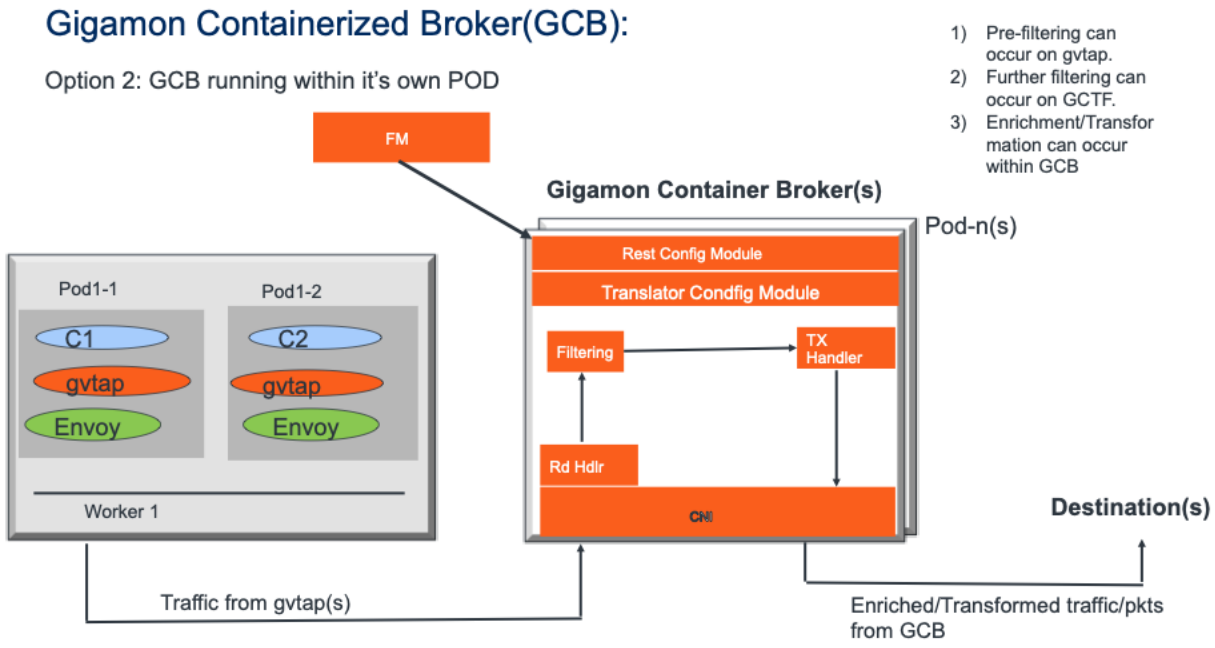
This chapter provides an overview of Gigamon containerized broker for cloud object storage and describes how to install and deploy G-vTAP Containers in your PODs.

Topics:

Architecture of Gigamon Containerized Broker for Cloud Object Storage

GCB with GigaVUE-FM deployment

With GCB in its own POD, you can choose an orchestrator (other than GigaVUE-FM) like K8S to spin up/down the GCB pods.



During GCB initialization, the GCB Controller tries to connect with the GigaVUE-FM IP that you provided in the YAML file. GigaVUE-FM have a server certificate and GCB have a client certificate, so that GigaVUE-FM and GCB can identify the connection and traffic flow. GigaVUE-FM doesn't control the GCB spin up/down. The GCB parameter definition and deployment is done through Kubernetes orchestrator and not by GigaVUE-FM.

Get Started with Gigamon Containerized Broker for Cloud Object Storage

This chapter describes how to initiate GCB deployment with the required licenses and network requisites.

Refer to the following sections for details:

- Components for Gigamon Containerized Broker for Cloud Object Storage
- License Information
- Network requirements

Components for Gigamon Containerized Broker for Cloud Object Storage

The Gigamon containerized broker for cloud object storage works with the following components:

- **GigaVUE® Fabric Manager (GigaVUE-FM)** is a web-based fabric management and orchestration interface that provides a single pane of glass visibility, management, and orchestration of both the physical and virtual traffic that form the GCB.
- **G-vTAP Container** is the Traffic Acquisition Component of Gigamon's Network Visibility Offering. It receives mirrored traffic from various Networking Infrastructures and overlays (VXLAN) them to Gigamon Containerized Broker.
- **GCB Controller** is the management component of GCB that controls the registration and deregistration with GigaVUE-FM. GCB Controller also sends the collected stats of GCB and G-vTAP Containers to GigaVUE-FM.
- **GCB S3** is the storage service component of GCB that collect the mirrored packets from GCB Controller, convert to PCAP file and upload it into Amazon S3.

License Information

All the G-vTAP instances connected to GCB periodically reports the stats to GCB. Then the GCB periodically reports the collective stats of G-vTAPs and its own stats to GigaVUE-FM for Volume-Based Licensing. GigaVUE-FM adds the required licensing tags into the Elasticsearch.

In the Volume-Based Licensing scheme, a license entitles specific applications on your devices to use a specified amount of total data volume over the term of the license. The distribution of the license to individual nodes or devices becomes irrelevant for Gigamon’s accounting purpose. GigaVUE-FM tracks the total amount of data processed by the various licensed applications and provides visibility into the actual amount of data, each licensed application is using on each node, and track the overuse if any.

Network requirements

A security group defines the virtual firewall rules for your instance to control inbound and outbound traffic. When you launch GigaVUE-FM, Gigamon Containerized Broker, and G-vTAP Containers in your project, you add rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic.

It is recommended to create a separate security group for each component using the rules and port numbers.

Direction	Type	Protocol	Port	CIDR	Purpose
Gigamon Containerized Broker deployed inside EKS worker node					
Inbound	HTTPS	TCP	443	Any IP address	Allows GCB Controller to communicate with GigaVUE-FM

Configure Gigamon Containerized Broker for Cloud Object Storage

This chapter describes how to configure GCB in your environment. Refer to the following section for details.

- Deploy G-vTAP Containers
- Launch GigaVUE-FM
- Launch Gigamon Containerized Broker
- Store traffic data in S3 bucket

Deploy G-vTAP Containers

Follow the below instructions to deploy G-vTAP Containers in your node:

1. In your Kubernetes orchestrator, enter the G-vTAP Container image name, commands and the required information in a YAML file. Following is the example data to be entered in the your YAML file:

```
image: gigamon/gvtap-container: :<version>
#imagePullPolicy: Never
#imagePullPolicy: Always
#imagePullPolicy: IfNotPresent
command: ["/gvtap", "1", "eth0", "eth0", "10.9.0.216", "4789", "45"]
```

2. Using the YAML file, Kubernetes automatically downloads the defined G-vTAP Container and deploys in the selected PODs in which traffic acquisition is required.

Launch GigaVUE-FM

The recent GigaVUE-FM image files can be downloaded from Gigamon Customer Portal. After fetching the image, upload and launch GigaVUE-FM inside or outside your VPC. For assistance, Contact Technical Support of Gigamon.

Launch Gigamon Containerized Broker

Follow the below instructions to deploy GCB in your node:

1. In your Kubernetes orchestrator, enter the GCB Controller and GCB S3 image name, commands and the required information in a YAML file. Following is the example data to be entered in the your YAML file:

```
image: gigamon/gcb-s3:<version>
- command:
- gcb-s3
- <pkt_filter_type(ip|tcp|udp)>
- <i_iface: eth0, eth1>
- <s3_bucket_name>(Ex: gcb_s3_bucket)
- <s3_region>(Ex: us-east-2>)
- <AWS Account-ID>
- <max_pkt_per_pcap>
- <idle_timeout (in sec)>
- <stats_active (0/1)>
- <gcm port>
- <stats_interval(in sec)>
- <filtering rule>
- <gcb vxlan port>

image: gigamon/gcb-cntlr:<version>
- command:
- /gcb-cntlr
- <GigaVUE-FM IP>
- <PORT ID for GCB controller to communicate with GigaVUE-FM>
```

2. Using the YAML file, Kubernetes automatically downloads the defined GCB Controller and GCB S3. Then both are deployed in a new POD.
3. Connect the deployed G-vTAP Containers to the GCB installed in the same node.
4. Register GCB with the GigaVUE-FM launched inside or outside your VPC.

Once the GCB is registered with GigaVUE-FM, the GCB starts to collect the traffic from the G-vTAP Containers and periodically sends the heartbeats and stats to GigaVUE-FM. For more information on GCB and GigaVUE-FM interaction, refer to Interaction between GCB and GigaVUE-FM

Store traffic data in S3 bucket

By default the traffic information from GCB is saved into Amazon S3 bucket. All the parameters of the S3 bucket are defined in the yaml files.

Following are the S3 bucket parameters defined in yaml file:

Parameter	Description
s3_bucket_name	Name of the Amazon S3 bucket
s3_region	AWS region (Example: us-east-2>)
AWS Account-ID	ID of AWS user account
max_pkt_per_pcap	Maximum packets required to create a PCAP file
idle_timeout (in sec)	Idle time limit to create PCAP file without waiting to collect the maximum packets defined.

Follow the below instructions to store the traffic data from GCB to your Amazon S3 bucket.

1. Save the traffic data from the GCB as a PCAP file with the Server Side Encryption technology.
2. Transfer and Save the encrypted PCAP files to your Amazon S3 bucket.

NOTE: Naming convention of the PCAP file and the folder in S3 bucket are as follows.

- PCAP file name: **<AWS Accout ID>_pod_<POD IP>_YYYY_MM_DD_HH_mm_ss_<milliseconds>.pcap**
- S3 folder name: **[S3 bucket name]/account_id/MM-DD-YYYY/[file-name]/**

View GCB statistics in GigaVUE-FM

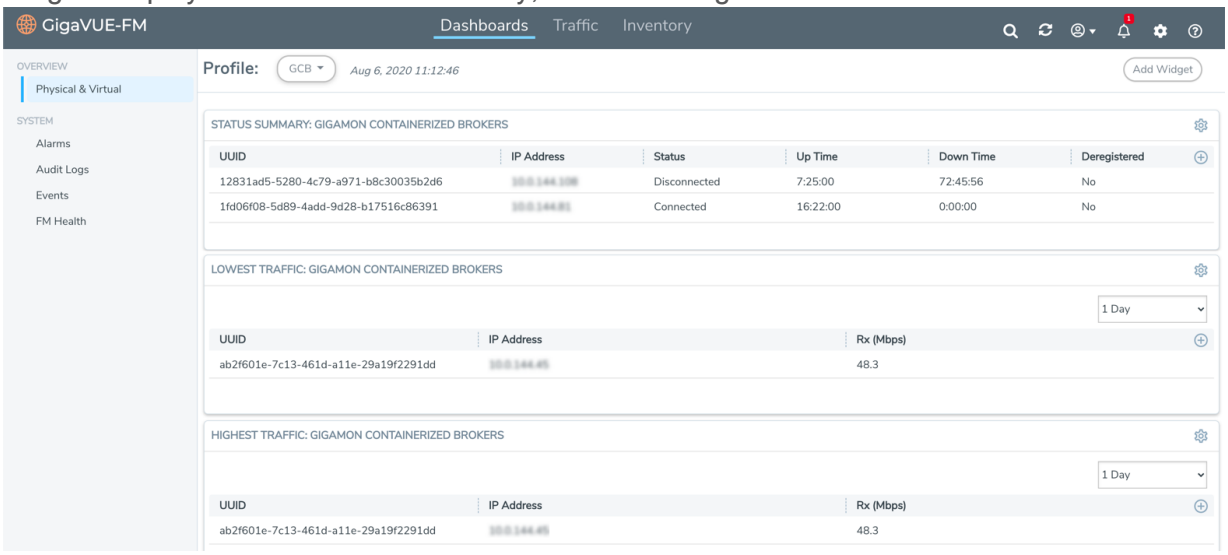
You can view the traffic information of GCB in GigaVUE-FM as the collective traffic from G-vTAPs and GCB are periodically transferred to GigaVUE-FM.

GigaVUE-FM dashboard displays the GCB stats in the following widgets:

- Status Summary
- Lowest Traffic
- Highest Traffic

To view the GCB stats in GigaVUE-FM:

1. On the top navigation bar, click **Dashboard**.
2. In the left navigation pane of the Dashboard page, click **Physical & Virtual**.
3. Click **Add Widget** and select Status Summary, Lowest Traffic, and Highest Traffic widgets. The widgets display the GCB status summary, lowest and highest traffic.



Gigamon Containerized Broker for Service Mesh and HTTPS/2 Support with Metadata

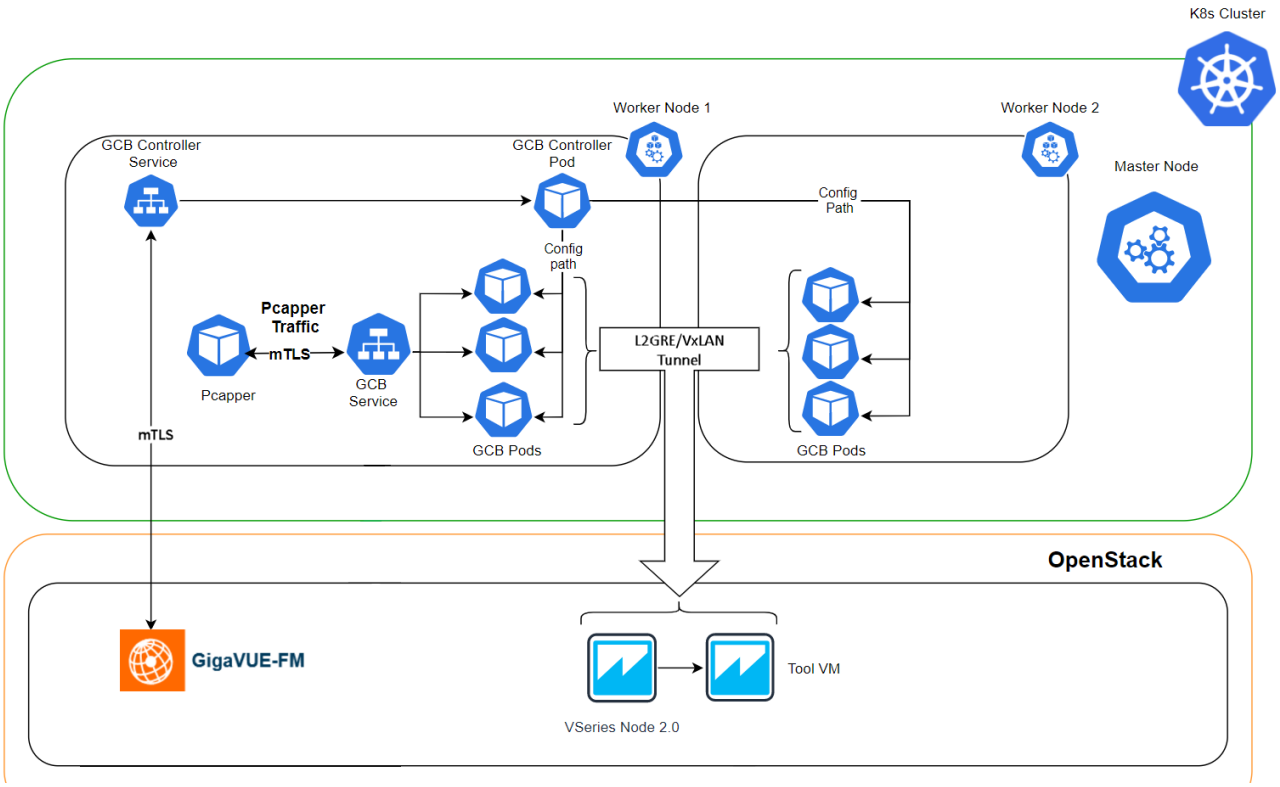
This guide provides an overview of Gigamon containerized broker for service mesh and HTTPS/2 support with metadata and describes how to install and deploy GCB components in your PODs.

Refer to the following topics for details:

- Architecture of Gigamon Containerized Broker for Service Mesh and HTTPS/2 Support with Metadata
- Get Started with Gigamon Containerized Broker for Service Mesh and HTTPS/2 Support with Metadata
- Configure GCB for Service Mesh and HTTPS/2 Support with Metadata through API

Architecture of Gigamon Containerized Broker for Service Mesh and HTTPS/2 Support with Metadata

The following diagram illustrates the architecture of Gigamon containerized broker for service mesh and HTTPS/2 support with metadata environment.



- The Pcapper collects the network traffic and sends the HTTPS packets to GCB service through mTLS authentication. Refer to Configure mTLS authentication for detailed information.
- In the GCB service, the received HTTP packets are load balanced across the available GCB Pods.
- GCB Pods filters the packets based on the metadata.
- The filtered HTTPS packets from GCB Pods are tunneled directly to the Tools or through the V Series nodes on OpenStack environment. Refer to the *GigaVUE Cloud Suite for OpenStack Configuration Guide* for more information on V Series configuration on OpenStack environment.
- GCB Controller collects the data from GCB Pods and sends the collected stats and heartbeats to GigaVUE-FM through mTLS authentication. Refer to Configure mTLS authentication for detailed information.

Get Started with Gigamon Containerized Broker for Service Mesh and HTTPS/2 Support with Metadata

This chapter describes how to initiate GCB and GigaVUE-FM deployment with the required licenses and network requisites.

Refer to the following sections for details:

- Components for Gigamon Containerized Broker
- License Information
- Network requirements

- Configure mTLS authentication

Components for Gigamon Containerized Broker

The Gigamon containerized broker for service mesh and HTTPS/2 support with metadata works with the following components:

- **GigaVUE® Fabric Manager (GigaVUE-FM)** is a web-based fabric management and orchestration interface that provides a single pane of glass visibility, management, and orchestration of both the physical and virtual traffic that form the GCB.
- **GCB Service** is traffic acquisition component that collects the data from the Pcapper and sends the the pcapper traffic to the GCB PODs.
- **GCB POD** is the primary GCB module that collects the pcapper traffic from GCB Service, filters the traffic and tunnels the filtered traffic directly to the tools or through the V Series nodes. GCB POD also sends the stats and heartbeats to GCB Controller.
- **GCB Controller** is the management component of GCB that is registered in GigaVUE-FM to control and communicate with GCB Pods. GCB Controller collects the data from GCB Pods and sends the collected stats and heartbeats to GigaVUE-FM.

License Information

All the GCB PODs deployed in your environment periodically reports the stats to GCB Controller. Then the GCB Controller periodically reports the collective stats of GCB PODs to GigaVUE-FM for Volume-Based Licensing. GigaVUE-FM adds the required licensing tags into the Elasticsearch.

In the Volume-Based Licensing scheme, a license entitles specific applications on your devices to use a specified amount of total data volume over the term of the license. The distribution of the license to individual nodes or devices becomes irrelevant for Gigamon's accounting purpose. GigaVUE-FM tracks the total amount of data processed by the various licensed applications and provides visibility into the actual amount of data, each licensed application is using on each POD, and track the overuse if any.

Network requirements

Following table describes the network requirements of GCB.

Direction	Type	Protocol	Port	CIDR	Purpose
Gigamon Containerized Broker deployed inside Kubernetes worker node					
Inbound	HTTPS	TCP	443	Any IP address	Allows GCB Controller to communicate with GigaVUE-FM
Inbound	HTTPS	TCP	8443(configurable)	Any IP address	Allows GigaVUE-FM to communicate with GCB Controller.

Configure mTLS authentication

Mutual TLS (mTLS) authentication or two-way authentication refers to the two parties (GigaVUE-FM & GCB, and Pcapper & GCB) authenticating each other at the same time in an authentication protocol. mTLS can protect against adversarial attacks and ensure information integrity.

GigaVUE-FM supports both mandatory mTLS and non-mandatory mTLS (basic authentication) using the username and password. Proper certificates need to be installed on both GigaVUE-FM and your environment, as default generated certificates will not work with mTLS.

> **NOTE:** During GigaVUE-FM upgrade, the files only with the **.crt** or **.key** under **/etc/pki/tls** extensions will be retained.

To configure mTLS authentication in GigaVUE-FM:

1. Log in to the GigaVUE-FM CLI.
2. Ensure that you have the following certificates and keys in the **/home/User/certsAndKeys** directory:
   - **fmServerCertificate.pem**: public certificate file in PEM format to be used by GigaVUE-FM when acting as a server.
   - **fmServerCertificateKey.pem**: private key file in PEM format to be used by GigaVUE-FM when acting as a server.
   - **fmServerCACertificate.pem**: public certificate file in PEM format of the CA which issued the fmServerCertificate.pem to be used by GigaVUE-FM when acting as a server.

     > **NOTE:** fmServerCACertificate.pem certificate needs to be imported into client's TrustStore, including browser if it is not issued by one of the trusted CAs.

   - **fmClientCertificate.pem**: public certificate file in PEM format to be used by GigaVUE-FM when acting as a client.
   - **fmClientCertificateKey.pem**: private key file in PEM format to be used by GigaVUE-FM when acting as a client.
   - **fmClientCACertificate.pem**: public certificate file in PEM format of the CA which issued the fmClientCertificate.pem to be used by GigaVUE-FM when acting as a client.

     > **NOTE:** If the same certificate is used when GigaVUE-FM is a client and as a server, the three **fmServer*.pem** files will be the same as the three **fmClient*.pem** files.

3. Change to the directory where the above files are stored.

   ```
   cd /home/User/certsAndKeys
   ```

4. Add **fmClientCACertificate.pem** to the GigaVUE-FM trust store:

   ```
   sudo cp fmClientCACertificate.pem   /etc/pki/ca-trust/source/anchors/

   sudo update-ca-trust extract
   ```

5. Install the certificates and private key to make GigaVUE-FM act as a server.
   a. Backup the existing certificate and copy new FM certificate **fmServerCertificate.pem**.

      ```
      sudo cp /etc/pki/tls/certs/localhost.crt
      /etc/pki/tls/certs/BACKUP_localhost.crt

      sudo cp fmServerCertificate.pem /etc/pki/tls/certs/localhost.crt
      ```

   b. Backup the existing private key and copy new GigaVUE-FM key **fmServerCertificateKey.pem**

      ```
      sudo cp /etc/pki/tls/private/localhost.key
      /etc/pki/tls/private/BACKUP_localhost.key

      sudo cp fmServerCertificateKey.pem
      /etc/pki/tls/private/localhost.key
      ```

      .
   c. GigaVUE-FM uses a public key (cms.p12 file) to encrypt the Security Assertion Markup Language (SAML) messages. Since for mTLS to work, we need valid certificates installed in FM, generate a new public key using the following command:

      ```
      sudo openssl pkcs12 -export -name CMS -out /etc/gigamon/cms.p12 \

      -inkey /etc/pki/tls/private/localhost.key -in
      /etc/pki/tls/certs/localhost.crt -passout pass:cms123
      ```

6. Install the certificates and private key to make GigaVUE-FM act as a client.
   a. Copy new client certificate **fmClientCertificate.pem**.

      ```
      sudo cp fmClientCertificate.pem
      /etc/pki/tls/certs/fmClientCertificate.crt
      ```

   b. Copy new client key **fmClientCertificateKey.pem**.

      ```
      sudo cp fmClientCertificateKey.pem
      /etc/pki/tls/private/fmClientCertificateKey.key
      ```

   c. Copy new client CA public certificate **fmClientCACertificate.pem**.

      NOTE: This certificate needs to be imported into GigaVUE-FM Trust Store.

      ```
      sudo cp fmClientCACertificate.pem
      /etc/pki/tls/certs/fmClientCACertificate.crt
      ```

7. Generate KeyStore for GigaVUE-FM to act as a client
   a. Create a client certificate chain file.

```
sudo cat /etc/pki/tls/certs/fmClientCACertificate.crt \

        /etc/pki/tls/certs/fmClientCertificate.crt \

        /etc/pki/tls/private/fmClientCertificateKey.key | sudo tee
/etc/pki/tls/certs/fmClient.chain.crt > /dev/null
```

   b. Create a client certificate chain file in PKCS12 format.

```
sudo openssl pkcs12 -export -in
/etc/pki/tls/certs/fmClient.chain.crt \

-out /etc/pki/tls/certs/fmClient.chain.p12 \

-passout pass:changeit
```

   c. Create Java keystore

```
sudo keytool -importkeystore -srckeystore
/etc/pki/tls/certs/fmClient.chain.p12 \

-srcstoretype pkcs12 \

-destkeystore /etc/pki/tls/certs/fmClientJKS.crt \

-storepass changeit
```

   d. Make the keystore readable.

```
sudo chmod 644/etc/pki/tls/certs/fmClientJKS.crt
```

   e. Restart Apache Web Server.

```
sudo systemctl restart httpd
```

   f. Restart the GigaVUE-FM.

```
sudo systemctl restart tomcat@cms.service
```

GigaVUE-FM is not responsible for any PKI or certificate management activities.

In a GigaVUE-FM High Availability (HA) environment, each GigaVUE-FM node will have a separate set of certificates (both client and server ones). If HA Proxy is used for GigaVUE-FM HA, then either HA proxy must run in TCP mode where mTLS will not be terminated by the HA Proxy server.

Configure GCB for Service Mesh and HTTPS/2 Support with Metadata

You can configure GCB through API or through GigaVUE-FM GUI. Refer to the following topics for detailed information.

- Configure GCB for Service Mesh and HTTPS/2 Support with Metadata through API
- Configure GCB for Service Mesh and HTTPS/2 Support with Metadata through GigaVUE-FM GUI

Configure GCB for Service Mesh and HTTPS/2 Support with Metadata through API

This chapter describes how to configure GCB and GigaVUE-FM in your environment through API. Refer to the following section for details.

- Launch GigaVUE-FM
- Deploy GCB Controller Service and GCB Controller PODs
- Deploy GCB Service and GCB PODs
- Configure Traffic Policy

Launch GigaVUE-FM

The recent GigaVUE-FM image files can be downloaded from Gigamon Customer Portal. After fetching the image, upload and launch GigaVUE-FM on your OpenStack environment. For assistance, Contact Technical Support of Gigamon or refer to the *GigaVUE Cloud Suite for OpenStack Configuration Guide* for more information on V Series configuration on OpenStack environment.

Deploy GCB Controller Service and GCB Controller PODs

Follow the below instructions to deploy GCB Controller Service and GCB Controller PODs in your node:

1. In your Kubernetes orchestrator, edit the GCB Controller image name, commands and the required information in a YAML file. Following is the example data to be entered in your YAML file:

```
name: gcb-cntlr
#image: gigamon/gcb-cntlr:<version>
#Usage:/gcb-cntlr <FM IP> <FM REST Svc Port> <GCB-Cntlr REST SVC Port>
command: [/gcb-cntlr, "12.345.67.890", '443' , '8443']
imagePullPolicy: Always
ports:
- containerPort: 8443
- containerPort: 42042
env:
- name: GCB_CNTLR_SERVICE_NAME
 value: "GIGAMON_GCB_CNTLR_SERVICE"
- name: GCB_CNTLR_EXT_IP_DNS
 value: "<external IP for GigaVUE-FM to reach GCB CNTLR"
- name: K8S_CLUSTER_ENDPOINT
 value: "https://<masternodeapiserverurl>:6443"
```

NOTE: The value of K8S_CLUSTER_ENDPOINT "https://<masternodeapiserverurl>:6443" must be same as the URL given during the connection creation.

```
- name: GCB_DEBUG_MODE
 value: "<hex value for debug>"
```

The hex value for GCB debugging must be in the **0x00[aaaa][b][c]** format, where

- aaaa is the number of pcaps
- b is 1 to create pcap and 0 is not to create pcap
- c is the log level ranges from 0 to 4

```
- name: GCB_CNTLR_POD_NAMESPACE
 valueFrom:
      fieldRef:
          fieldPath: metadata.namespace
```

2. Using the YAML file, Kubernetes automatically downloads the defined GCB Controller and deploys in the selected PODs in which traffic acquisition is required.

Deploy GCB Service and GCB PODs

Follow the below instructions to deploy GCB service and GCB PODs in your node:

1. In your Kubernetes orchestrator, edit the GCB Service and GCB POD image name, commands and the required information in a YAML file. Following is the example data to be entered in your YAML file:

```
name: gcb-http
command:
#gcb-http PORT mTLS-Flag(T/F) CERT_FILE KEY_FILE CA_CERT_FILE CA_VERIFY
(T/F)
- /gcb-http
- "9443" <HTTP Port Number for ingress traffic>
- "true" <Create a certificate (T/F)>
- "server-certificate-chain.pem" <SSL/TLS certificates>
- "server-private-key.pem"<Private key for the certificate>
- "ca-root-crt-chain.crt" <CA root certificate>
- "false"
- "10.244.2.132" <Default Destination IP>
- "0" <(0/1) Enter 1 to use the default destination IP, or enter 0 to
use the rules configured by GigaVUE-FM>
#image: gigamon/gcb-http:<version>
imagePullPolicy: Always
env:
- name: GCB_SERVICE_NAME
  value: "GIGAMON_GCB_HTTP2_SERVICE"
- name: GCB_CNTLR_SVC_DNS <GCB Controller Service Number>
  #value: "<GCB-CNTLR-SVC-NAME.GCB-CNTLR-NAMESPACE>.svc.cluster.local"
  value: "gigamon-gcb-cntlr-service.default.svc.cluster.local"
- name: GCB_CNTLR_REST_SVC_PORT
  value: '8443'
- name: GCB_POD_NAMESPACE
  valueFrom:
      fieldRef:
          fieldPath: metadata.namespace
```

2. Using the YAML file, Kubernetes automatically downloads and deploys the defined GCB Service and GCB POD.

Configure Traffic Policy

Once the GCB Controller is registered with GigaVUE-FM and the traffic policy is deployed to GCBs, then the GCB starts to collect the traffic and stats periodically sends the heartbeats and stats to GigaVUE-FM. For more information on GCB and GigaVUE-FM interaction, refer to Interaction between GCB and GigaVUE-FM

Configure GCB for Service Mesh and HTTPS/2 Support with Metadata through GigaVUE-FM GUI

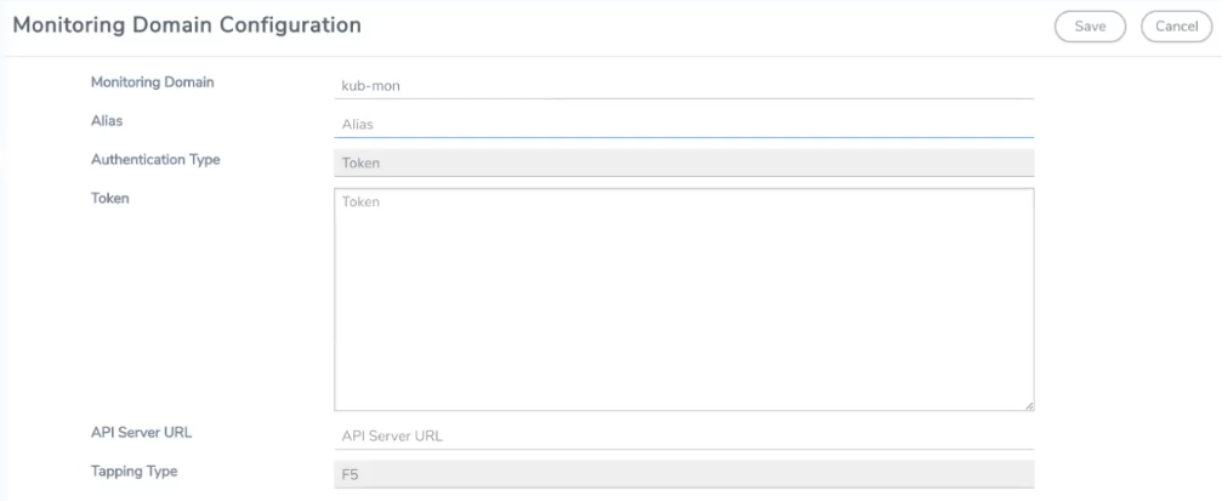
This chapter describes how to configure GCB through GigaVUE-FM GUI. Refer to the following section for details.

- Create a monitoring domain
- Configure Traffic Policy

Create a monitoring domain

To create a monitoring domain in GigaVUE-FM:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > VIRTUAL > Orchestrated Flows > KubernetesGCB > Monitoring Domain**. The **Monitoring Domain** page appears.
2. In the Monitoring Domain page, click **New**. The Monitoring Domain Configuration wizard appears.



3. Enter or select the required information as described in the following table,

Fields	Description
Monitoring Domain	Enter a name for the monitoring domain.
Alias	Enter a name for the GCB connection.
Authentication Type	Select Token as the authentication type.
Token	-
API Server URL	Enter the URL of the API server
Tapping Type	Select **F5** as the Tapping Type

4. Click **Save** to create a monitoring domain.

NOTE: After creating a monitoring domain, you must add F5 field information through REST API. Refer to Monitoring Domain and Traffic Policy Configuration.

Configure Traffic Policy

To create a Traffic Policy in GigaVUE-FM:

1. After adding F5 field information, in GigaVUE-FM left navigation pane, select **Inventory > VIRTUAL > Orchestrated Flows > KubernetesGCB**. The **Orchestrate** page appears with the **Traffic Policy** tab.
2. In the Traffic Policy tab, click **Create**. The Create Tunnels and Rules wizard appears.
3. In the **Tunnels** tab, enter or select the required information as described in the following table,

Fields	Description
Tunnel Name	Enter a name for the Tunnel.
Remote IP Address	Enter an IP Address for the Tunnel.
Tunnel Type	Select L2GRE or VXLAN as the tunnel type.
Tunnel Key	Enter a value for the tunnel key.
Destination Port	Enter the tool destination port number.

4. Switch to Rules tab, and enter or select the required information as described in the following table:

Fields	Description
Policy	
Policy Name	Enter a name for the policy.
Connection	Select a connection for the policy.
Rules	
Name	Enter a name for the Rule.
Destination Name	Select a tunnel destination.
Pass/Drop	Select Pass to allow the packets or select Drop to block the packets based on the filters.
Filter type	Select a filter type that you posted in F5 fields.
Filter value	Enter a value for the filter type.

5. Click **Create** and this new Traffic Policy deploys itself in the GCB.

The Traffic Policy processes the pcapper traffic and forwards the traffic to the tunnel destination IP address.

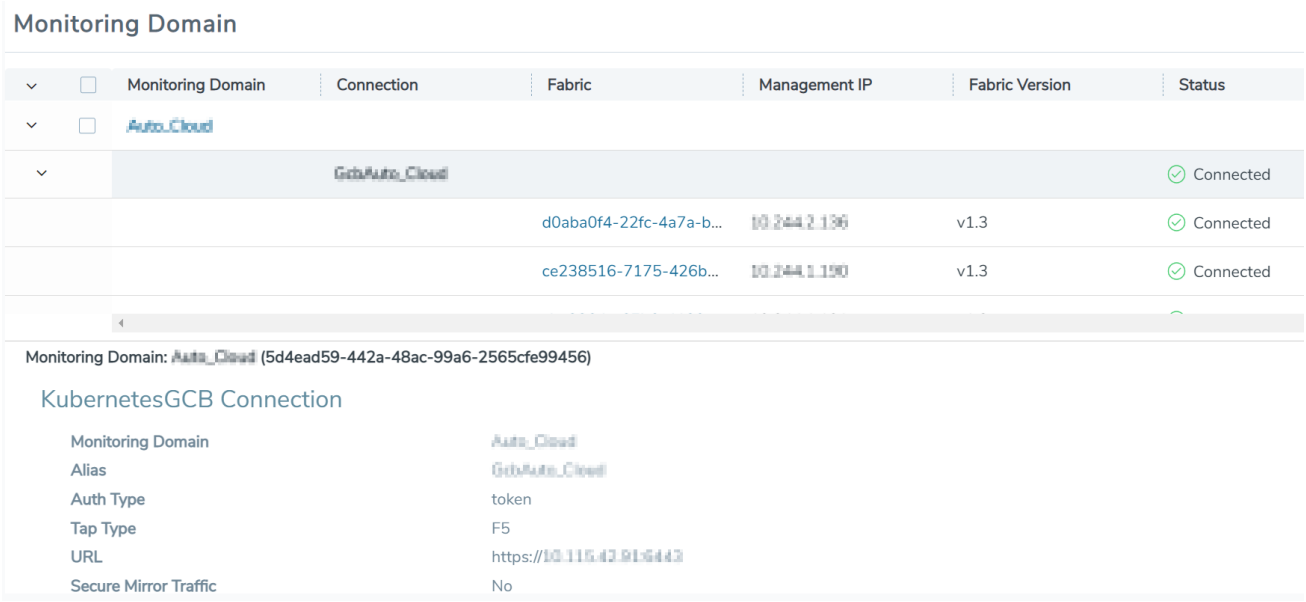
View GCB Specifications in GigaVUE-FM

You can view the following GCB specifications in GigaVUE-FM:

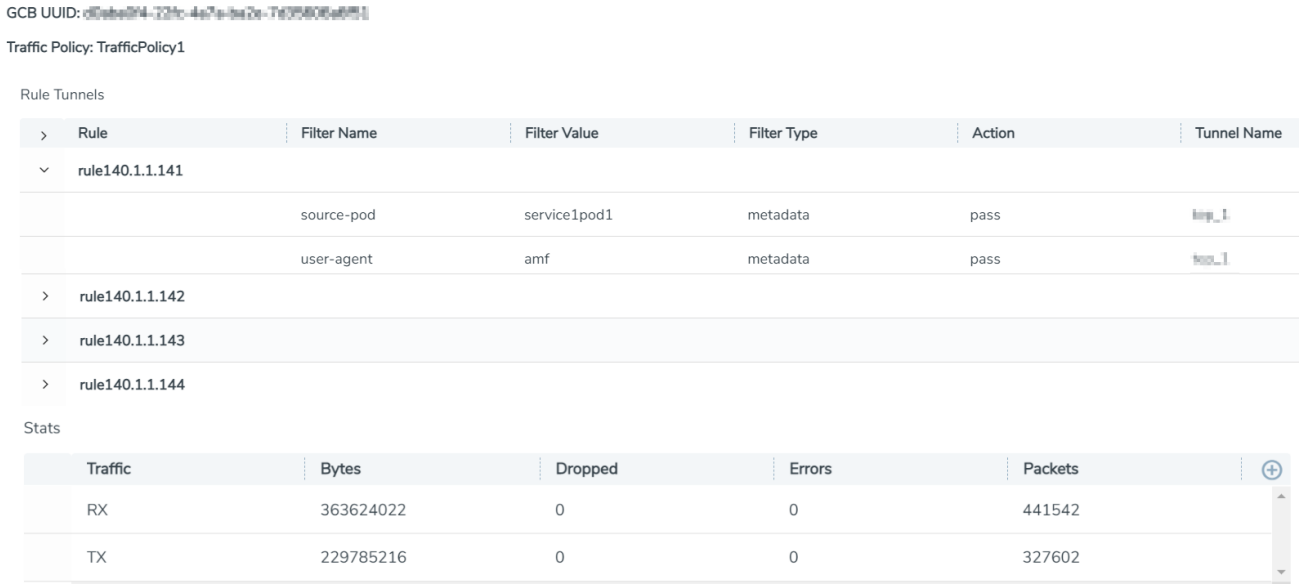
View GCB Monitoring Domain

To view the Monitoring Domains of GCB in GigaVUE-FM, navigate to **Inventory > VIRTUAL > KubernetesGCB > Monitoring Domain**. The Traffic Policy page appears with the list of Traffic Policies. You can add, edit, or delete the Monitoring Domains of GCB only through GigaVUE-FM REST APIs but not through GigaVUE-FM GUI.

In the Monitoring Domains list, click on a Monitoring Domain name to view the details of the selected Monitoring Domain.

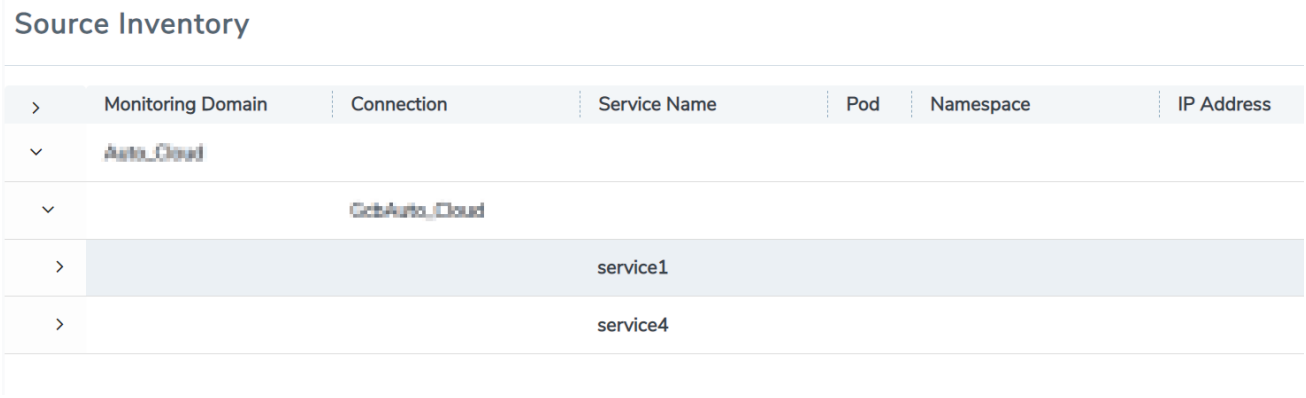


From any existing Monitoring Domain cluster, click on a GCB fabric to view the Rule Tunnels and Stats.



View Source Inventory

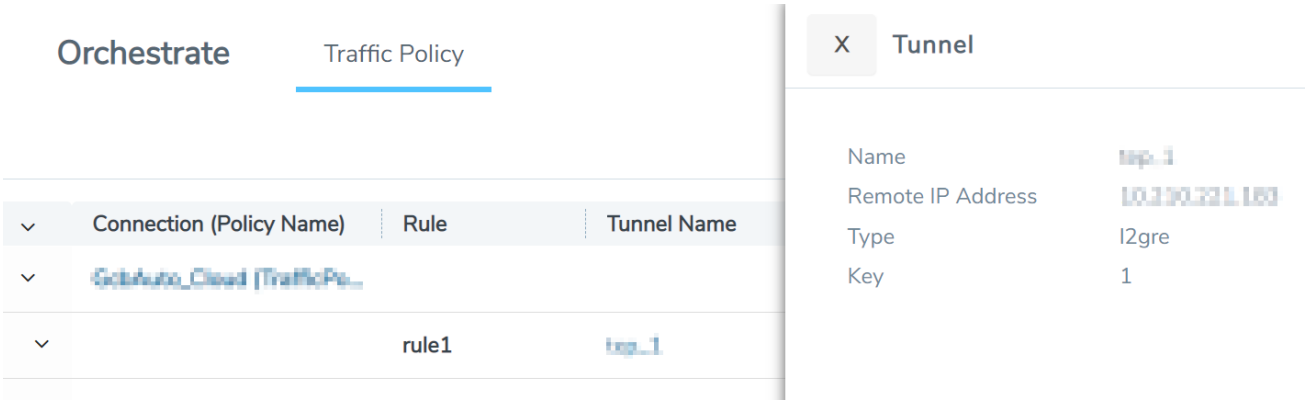
To view the Kubernetes Cluster Source Inventory of GCB in GigaVUE-FM, navigate to **Inventory > VIRTUAL > KubernetesGCB > Source Inventory**. The Source Inventory page appears with the list of Kubernetes cluster inventories. You can add, edit, or delete the Source Inventory of Kubernetes clusters only through REST APIs but not through GigaVUE-FM GUI.



View GCB Traffic Policy

To view the Traffic Policies (Monitoring Sessions) of GCB in GigaVUE-FM, navigate to **Traffic > VIRTUAL > Orchestrated Flows > KubernetesGCB**. The Traffic Policy page appears with the list of Traffic Policies. You cannot add, edit, or delete the Traffic policies only through REST APIs but not through GigaVUE-FM GUI.

From any existing Traffic Policy, click on the Tunnel Name. The Tunnel quick view appears with the details of the selected tunnel.



Click on the Connection (Policy Name) to view the status of the last operation performed on the policy.

Additional Sources of Information

This appendix provides additional sources of information. Refer to the following sections for details:

- Documentation
- Documentation Feedback
- Contact Technical Support
- Contact Sales
- The Gigamon Community

Documentation

This table lists all the guides provided for GigaVUE Cloud Suite software and hardware. The first row provides an All-Documents Zip file that contains all the guides in the set for the release.

NOTE: In the online documentation, view What's New to access quick links to topics for each of the new features in this Release; view Documentation Downloads to download all PDFs.

Table 1: Documentation Set for Gigamon Products

GigaVUE Cloud Suite 5.12 Hardware and Software Guides
DID YOU KNOW? If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing **Edit > Advanced Search** from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.
Hardware how to unpack, assemble, rack-mount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices
*G-TAP A Series 2 Installation Guide
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC2 Hardware Installation Guide
GigaVUE-HC3 Hardware Installation Guide
GigaVUE M Series Hardware Installation Guide
GigaVUE TA Series Hardware Installation Guide
*GigaVUE-OS Installation Guide for DELL S4112F-ON
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
GigaVUE-OS Upgrade Guide

GigaVUE Cloud Suite 5.12 Hardware and Software Guides
Administration
GigaVUE Administration Guide covers both GigaVUE-OS and GigaVUE-FM
Fabric Management
GigaVUE Fabric Management Guide how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
Cloud Configuration and Monitoring how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms
GigaVUE Cloud Suite for AnyCloud Configuration Guide how to deploy the GigaVUE Cloud Suite solution in any cloud platform
GigaVUE Cloud Suite for AWS Configuration Guide
GigaVUE Cloud Suite for AWS Quick Start Guide quick view of AWS deployment
GigaVUE Cloud Suite for AWS SecretRegions Configuration Guide
GigaVUE Cloud Suite for Azure Configuration Guide
GigaVUE Cloud Suite for Kubernetes Configuration Guide
GigaVUE Cloud Suite for Nutanix Configuration Guide
GigaVUE Cloud Suite for OpenStack Configuration Guide
GigaVUE Cloud Suite for VMware Configuration Guide
Gigamon Containerized Broker
Reference
GigaVUE-OS-CLI Reference Guide library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE H Series and TA Series devices
GigaVUE-OS Cabling Quick Reference Guide guidelines for the different types of cables used to connect Gigamon devices
GigaVUE-OS Compatibility and Interoperability Matrix compatibility information and interoperability requirements for Gigamon devices
GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide samples uses of the GigaVUE-FM Application Program Interfaces (APIs)
Release Notes

GigaVUE Cloud Suite 5.12 Hardware and Software Guides
GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes new features, resolved issues, and known issues in this release ; important notes regarding installing and upgrading to this release **NOTE:** Release Notes are not included in the online documentation. **NOTE:** Registered Customers can log in to My Gigamon to download the Software and Release Notes from the Software & Docs page on to My Gigamon. Refer to How to Download Software and Release Notes from My Gigamon.
In-Product Help
GigaVUE-FM Online Help how to install, deploy, and operate GigaVUE-FM.
GigaVUE-OS H-VUE Online Help provides links the online documentation.

How to Download Software and Release Notes from My Gigamon

Registered Customers can download software and corresponding Release Notes documents from the **Software & Release Notes** page on to My Gigamon. Use the My Gigamon Software & Docs page to download:

- Gigamon Software installation and upgrade images,
- Release Notes for Gigamon Software, or
- Older versions of PDFs (pre-v5.7).

To download release-specific software, release notes, or older PDFs:

1. Log in to My Gigamon
2. Click on the **Software & Release Notes** link.
3. Use the **Product** and **Release** filters to find documentation for the current release. For example, select Product: "GigaVUE-FM" and Release: "5.6," enter "pdf" in the search box, and then click **GO** to view all PDF documentation for GigaVUE-FM 5.6.xx.

NOTE: My Gigamon is available to registered customers only. Newer documentation PDFs, with the exception of release notes, are all available through the publicly available online documentation.

Documentation Feedback

We are continuously improving our documentation to make it more accessible while maintaining accuracy and ease of use. Your feedback helps us to improve. To provide feedback and report issues in our documentation, send an email to: documentationfeedback@gigamon.com

Please provide the following information in the email to help us identify and resolve the issue. Copy and paste this form into your email, complete it as able, and send. We will respond as soon as possible.

Documentation Feedback Form		
About You	Your Name	
	Your Role	
	Your Company	
For Online Topics	Online doc link	*(URL for where the issue is)*
	Topic Heading	*(if it's a long topic, please provide the heading of the section where the issue is)*
For PDF Topics	Document Title	*(shown on the cover page or in page header)*
	Product Version	*(shown on the cover page)*
	Document Version	*(shown on the cover page)*
	Chapter Heading	*(shown in footer)*
	PDF page #	*(shown in footer)*
How can we improve?	Describe the issue	*Describe the error or issue in the documentation.* *(If it helps, attach an image to show the issue.)*
	How can we improve the content? Be as specific as possible.	
	Any other comments?	

Contact Technical Support

See https://www.gigamon.com/support-and-services/contact-support for Technical Support hours and contact information. You can also email Technical Support at support@gigamon.com.

Contact Sales

Use the following information to Gigamon channel partner or Gigamon sales representatives.

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

Email Gigamon at inside.sales@gigamon.com for information on purchasing 24x7 Premium Support. Premium Support entitles you to round-the-clock phone support with a dedicated Support Engineer every day of the week.

The Gigamon Community

The Gigamon Community is a technical site where Gigamon users, partners, security and network professionals and Gigamon employees come together to share knowledge and expertise, ask questions, build their network and learn about best practices for Gigamon products.

Visit the Gigamon Community site to:

- Find knowledge base articles and documentation
- Ask and answer questions and learn best practices from other members.
- Join special-interest groups to have focused collaboration around a technology, use-case, vertical market or beta release
- Take online learning lessons and tutorials to broaden your knowledge of Gigamon products.
- Submit and vote on feature enhancements and share product feedback. (Customers only)
- Open support tickets (Customers only)
- Download the latest product updates and documentation (Customers only)

The Gigamon Community is a great way to get answers fast, learn from experts and collaborate directly with other members around your areas of interest.

Register today at community.gigamon.com

Questions? Contact our Community team at community@gigamon.com.